# Deploying Mobile Access Server

## Session 617

These are confidential sessions—please refrain from streaming, blogging, or taking pictures.

# Deploying Mobile Access Server

**Steve Cervera,** Solutions Architect Manager
**Al Begley,** Software Engineer
**John Murata,** Software Engineer
**Greg Vaughan,** Software Engineer

# Agenda

- What is Mobile Access Server?
- What problem does it solve?
- How it works
- Deployment strategies
- Demo
- Q & A

# Mobile Access from Anywhere

# Mobile Access from Anywhere

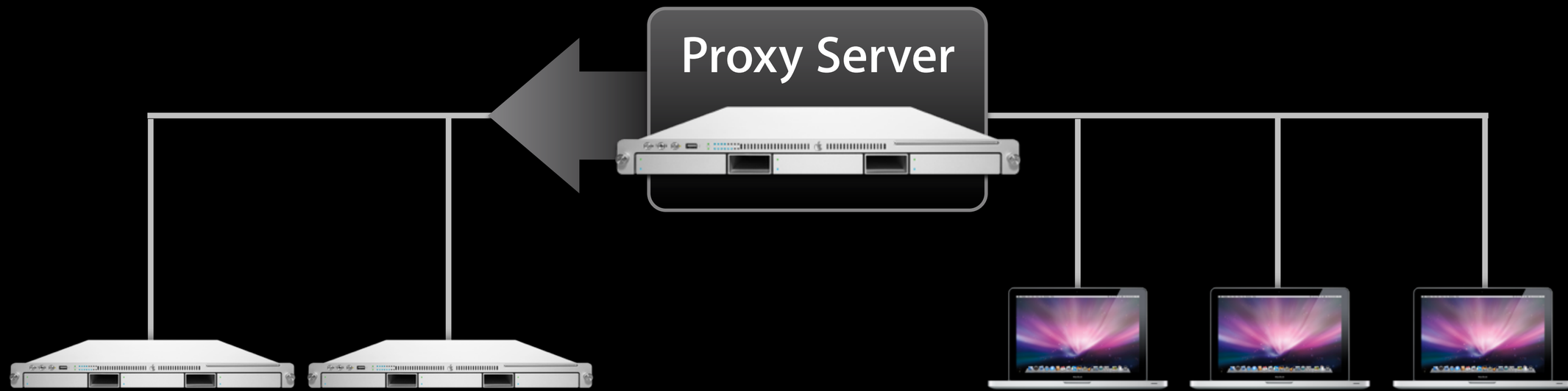
# What Is Mobile Access Server?

- Provides secure access to
  - Wiki server (other web services)
  - Mail server
  - iCal server
  - Address Book server
- Eliminates the need for VPN
- Communication encrypted with SSL
- Allows access only to specified servers and services by authorized users

# What Is Mobile Access Server?

- Easy to configure and administer
- Easy to connect through; no client configuration
- Enables single name space access from both internal and external networks
- Can also be used with laptops and iPod Touch

# HTTP “Forward” Proxy



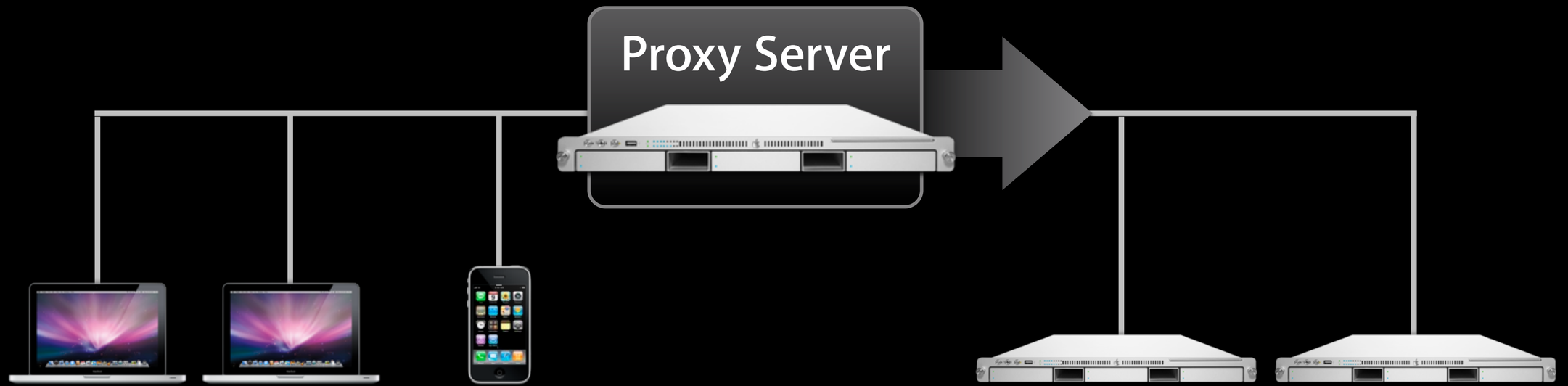

External Network

Internal Network

Typical Uses:

- Access from Intranet to Internet
- Improve responsiveness via cache
- Optimize use of bandwidth
- Control access to internet

# HTTP “Reverse” Proxy



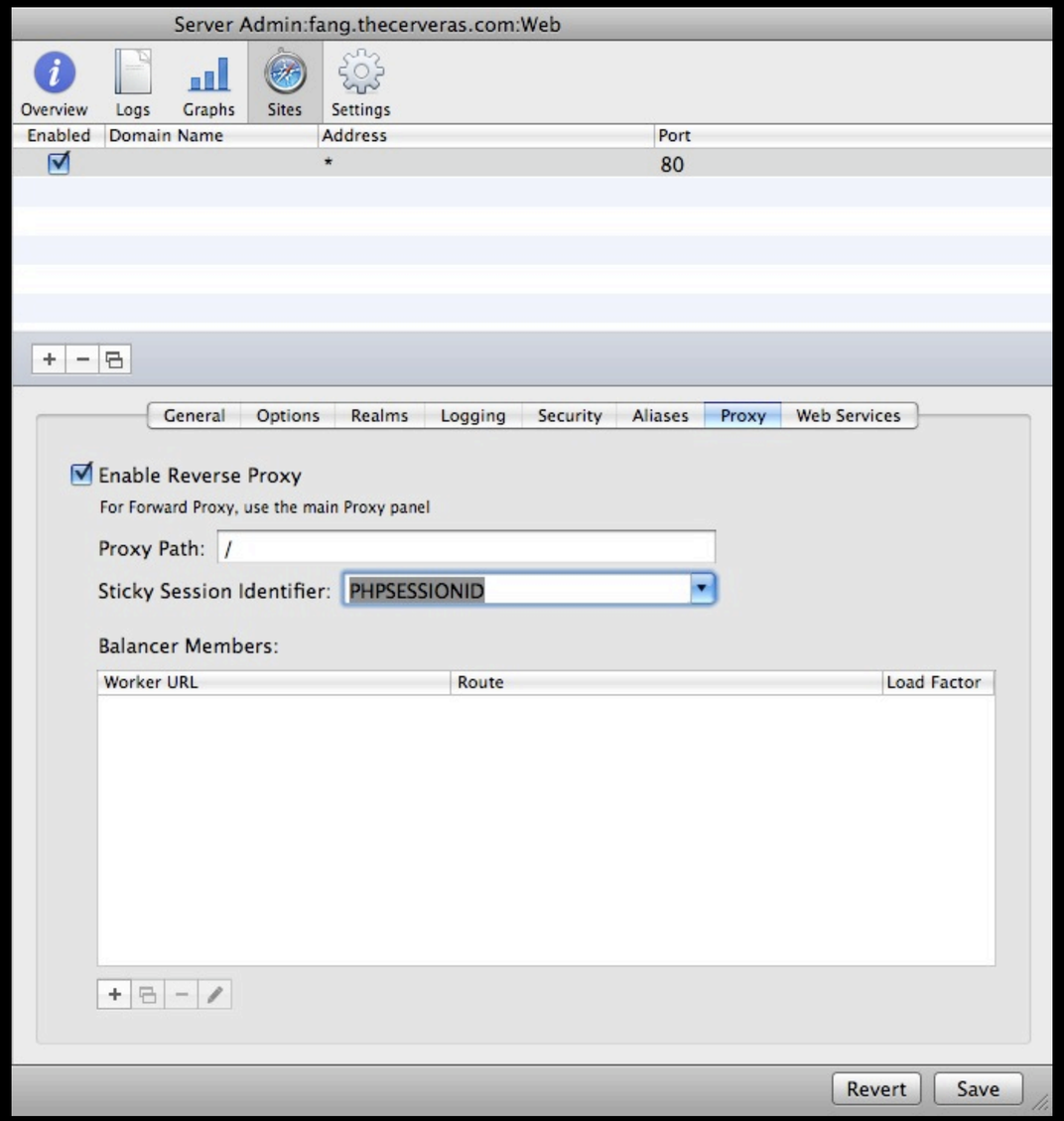

External Network

Internal Network

Typical Uses:

- Access from Internet to Intranet
- Security layer
- Load balancing

# Introduced in Leopard Server



# Common Reverse Proxy Schemes

- Modified host name, constant path
- Modified host name, modified path
- Constant host name, constant path, split DNS

# Defining Terminology

External Network

Internal Network

Client

Proxy Server

**Origin Server**
wiki.example.com

# Common Reverse Proxy

## Modified host name, constant path

External Network

ISP DNS

Client

wikiproxy.example.com
63.x.y.z

wikiproxy

Internal Network

DNS

**Origin Server**
wiki.example.com
172.24.240.5

# Common Reverse Proxy

## Modified host name, modified path

External Network

ISP DNS

Client

wikiproxy.example.com/wiki
63.x.y.z

wikiproxy

Internal Network

DNS

**Origin Server**
wiki.example.com
172.24.240.5

# Split DNS and Reverse Proxy

## Constant host name, constant path, split DNS

External Network

Internal Network

ISP DNS

DNS

wiki.example.com
63.x.y.z

Client

Mobile
Access Server

Origin Server
wiki.example.com
172.24.240.5

# Split DNS and Reverse Proxy

## Constant host name, constant path, split DNS

External Network

ISP DNS

Internal Network

DNS

wiki.example.com
63.x.y.z

**Mobile Access Server**

I'm making bookmarks

**Origin Server**
wiki.example.com
172.24.240.5

My
web apps
work too!

# Split DNS

- Mobile Access Server is multihomed in DMZ
- Internal DNS server resolves host name to the internal IP address of origin server, bypassing Mobile Access Server
- DNS from ISP resolves host name of origin server to externally facing IP of the Mobile Access Server
  - External DNS Servers
    - wiki.example.com = 63.x.y.z
  - Internal DNS Server
    - wiki.example.com = 172.24.240.5

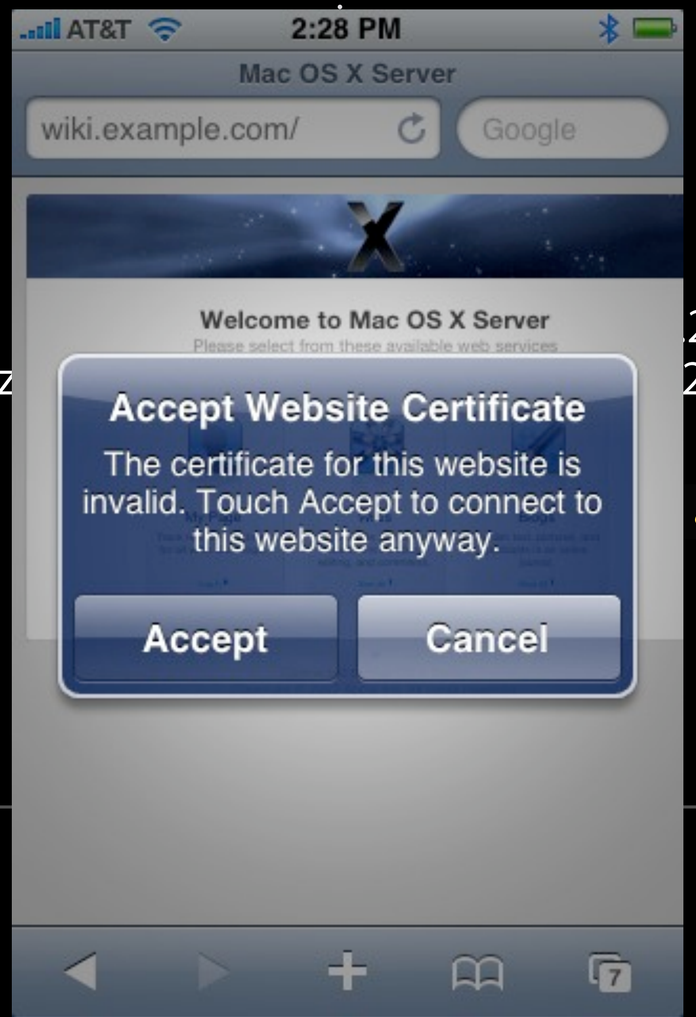
# Firewall Rules and Certificates

External Network

ISP DNS

Any to 63.x.y.z

http://wiki.example.com




.24.240.1

24.240.5

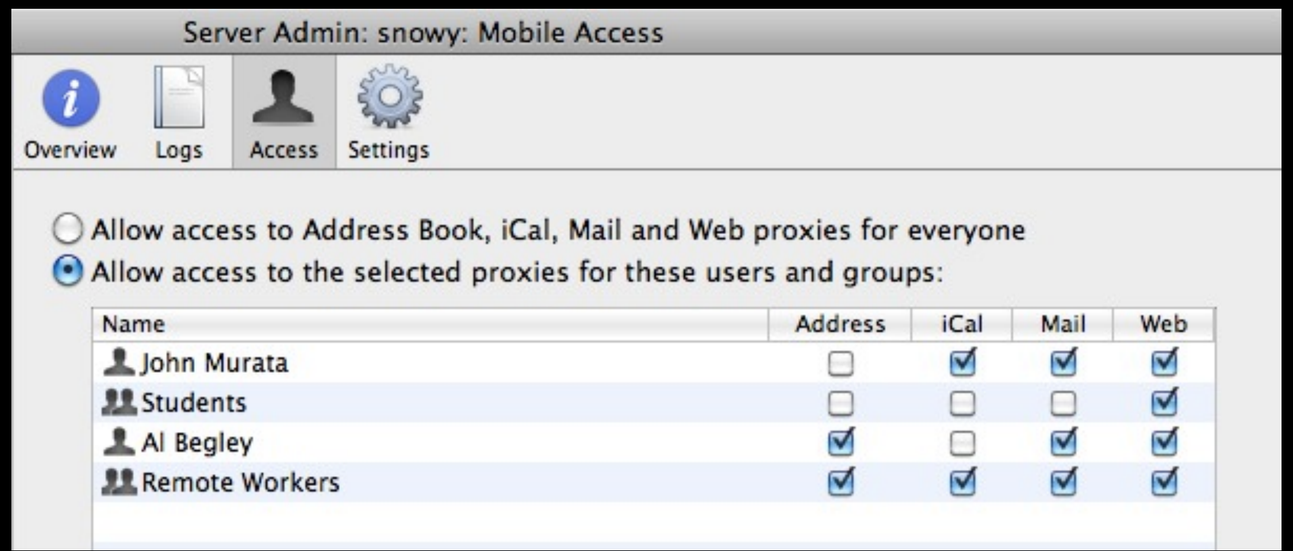
Internal Network

DNS

wiki.example.com
172.24.240.5

# Security

- All data is encrypted over SSL from client to proxy
- Access through Mobile Access server requires Authentication to OD/AD
- Repeated failed attempts incur increasing delays
- Authorization via “whitelist”
  - User ID and/or group membership
  - Per service type: iCal, AddressBook, Wiki, Mail



# Three Access Mechanisms

## HTTP/HTTPS

## IMAP/SMTP

# Three Access Mechanisms

# Controlling Access

- Apache Plugin mod_auth_session_apple
- Web server only
- Provides login UI
- Redirects failure to “Access Denied” URL
  - Try again
  - “Auth throttle back”
- Redirects successful login to requested URL
- “Keep me logged in”: Session ID expires in 14 days

# Web Services Via Mobile Access Server

External Network

Internal Network

SSL
https

Mobile Access Server
63.x.y.z
wiki.example.com

wiki.example.com

# Web Services Via Mobile Access Server

External Network

Internal Network

SSL
https

Mobile Access Server
63.x.y.z
wiki.example.com

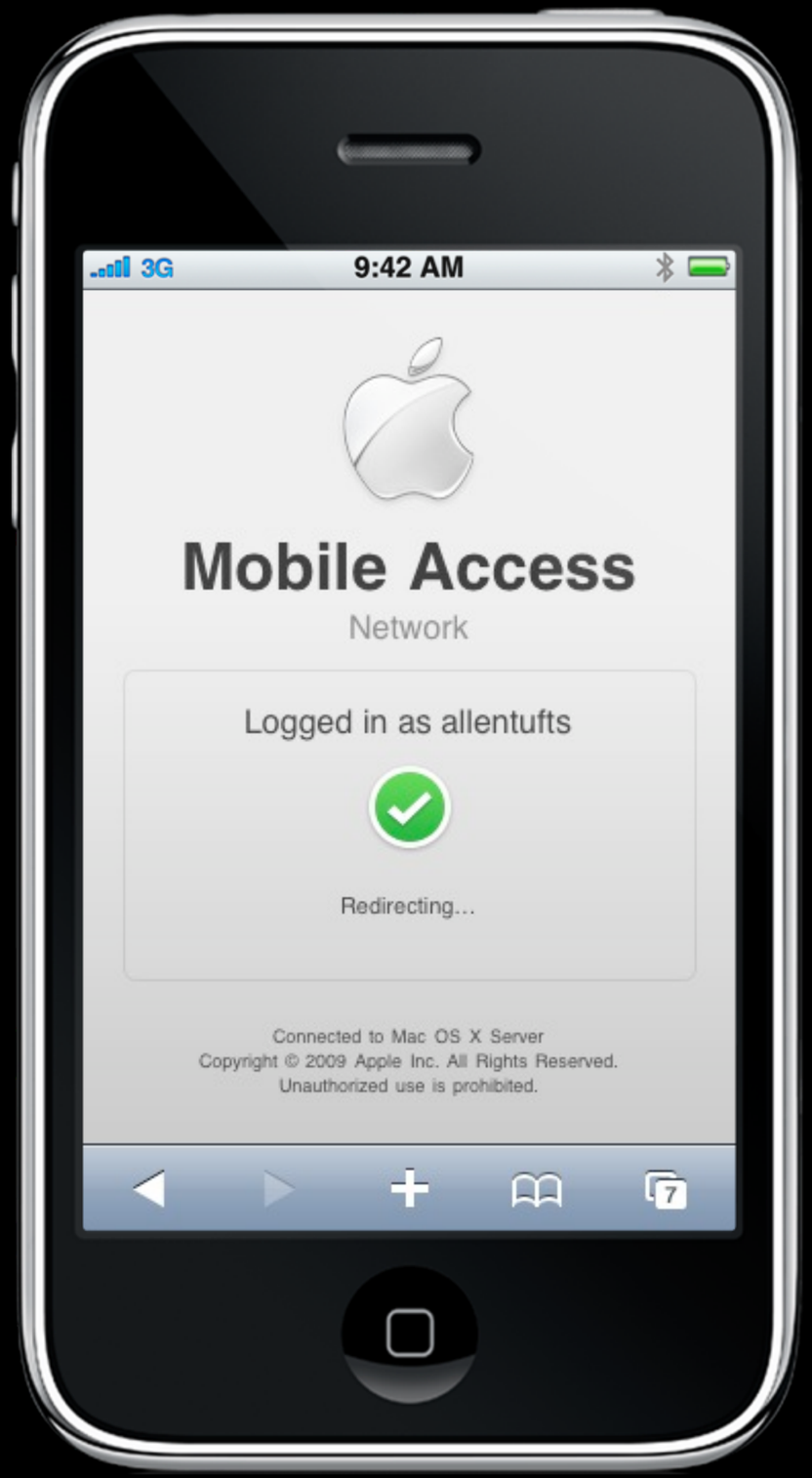
wiki.example.com

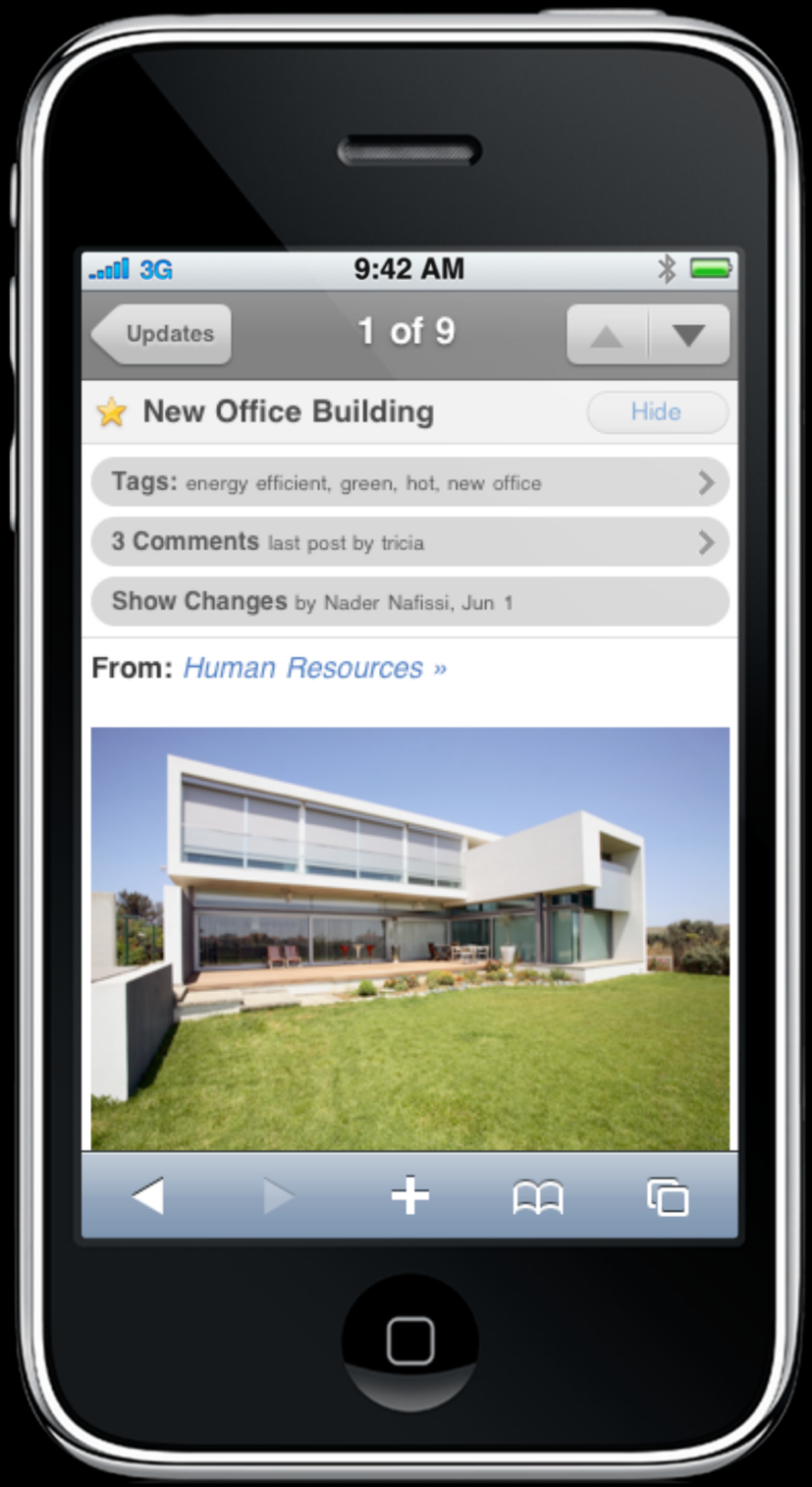
3G
9:42 AM
Mac OS X Server
Cancel
http://wiki.example.com/
Welcome to Mac OS X Server
Please select from these available web services
My Page
Wikis
Blogs
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
@123
.
/
.com
Go

3G
9:42 AM
Mobile Access
Network
user name
password
keep me logged in
Log in
Connected to Mac OS X Server
Copyright © 2009 Apple Inc. All Rights Reserved.
Unauthorized use is prohibited.

3G
9:42 AM
Mobile Access
Network
allentufts
keep me logged in
Log in
Connected to Mac OS X Server
Copyright © 2009 Apple Inc. All Rights Reserved.
Unauthorized use is prohibited.

3G
9:42 AM
Mobile Access
Network
Access denied
Try again
Connected to Mac OS X Server
Copyright © 2009 Apple Inc. All Rights Reserved.
Unauthorized use is prohibited.


3G
9:42 AM
Mobile Access
Network
Logged in as allentufts
Redirecting...
Connected to Mac OS X Server
Copyright © 2009 Apple Inc. All Rights Reserved.
Unauthorized use is prohibited.


3G
9:42 AM
Updates
1 of 9
New Office Building
Hide
Tags: energy efficient, green, hot, new office
3 Comments last post by tricia
Show Changes by Nader Nafissi, Jun 1
From: Human Resources »

3G
9:42 AM
Mobile Access
Network
Mobile Access is not available.
Try again
Connected to Mac OS X Server
Copyright © 2009 Apple Inc. All Rights Reserved.
Unauthorized use is prohibited.

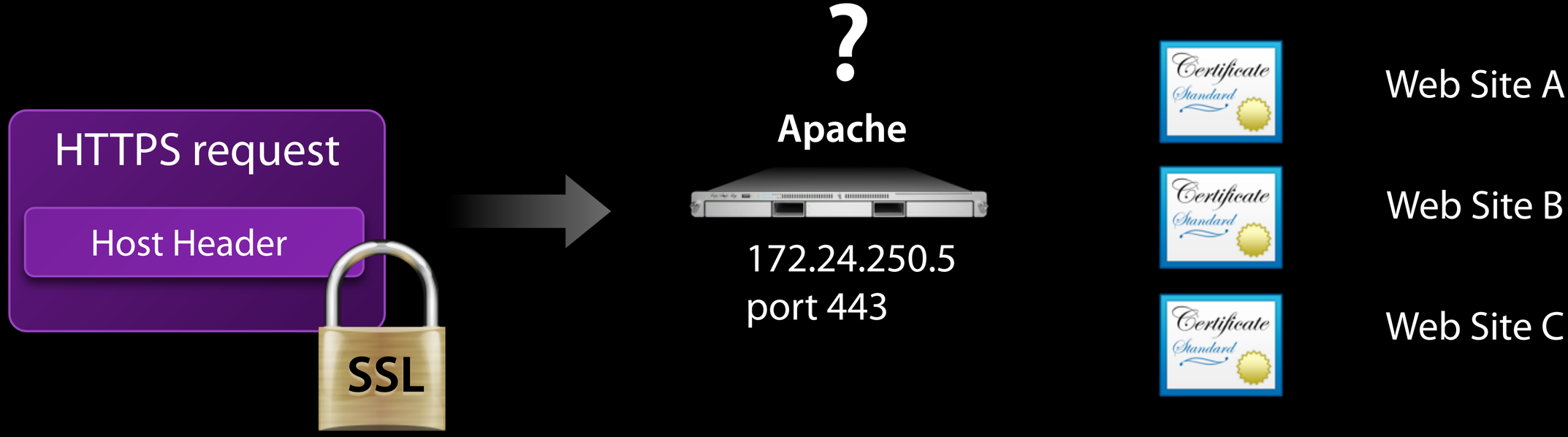
# Web Proxy Compatibility

## Web Apps

- X-Forwarded-for Header—contains actual client IP address
- Relative links
- Link to proxied or public hosts
- Web servers can use Basic, Digest, or session-cookie authentication , but not Kerberos

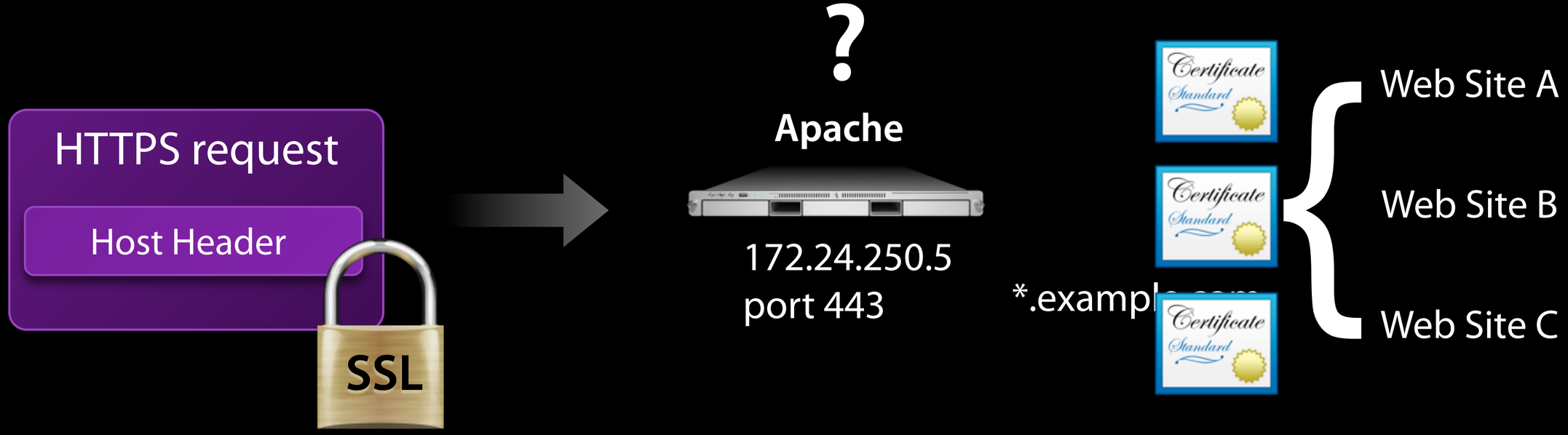
# Name-Based Virtual Hosts vs. SSL

- Host Header not part of SSL handshake
  - Normally requires IP-specific virtual hosts



# Name-Based Virtual Hosts vs. SSL

- Host Header not part of SSL handshake
  - Normally requires IP-specific virtual hosts
- Solutions:
  - Wild-card certificate



# Name-Based Virtual Hosts vs. SSL

- Host Header not part of SSL handshake
  - Normally requires IP-specific virtual hosts
- Solutions:
  - Wild-card certificate
- Port-specific virtual hosts

# Name-Based Virtual Hosts vs. SSL

- Host Header not part of SSL handshake
  - Normally requires IP-specific virtual hosts
- Solutions:
  - Wild-card certificate
- Port-specific virtual hosts
- Manually edit virtual host config files to be IP specific (discouraged)

Terminal — ssh — 87×12

```
## Default Virtual Host Configuration

<VirtualHost *:80>
        ServerAdmin admin@example.com
        DocumentRoot "/Library/WebServer/Documents"
        DirectoryIndex index.html index.php
        CustomLog "/var/log/apache2/access_log" "%h %l %u %t \"%r\" %>s %b"
        ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
        <IfModule mod_ssl.c>
                SSLEngine Off
                SSLCipherSuite "ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"
                SSLProtocol -ALL +SSLv3 +TLSv1
```

# Three Access Mechanisms

## HTTP/HTTPS

## IMAP/SMTP

# Three Access Mechanisms

# Controlling Access

- Apache Plugin mod_auth_user_host_apple
  - Authorization only
- iCal Server and Address Book Server does authentication
- Extracts user name from HTTP Authorization headers
  - Basic or Digest authentication, no Kerberos
- Checks user name against whitelist for requested service

# iCal and Address Book Services Via Mobile Access Server

External Network

Internal Network

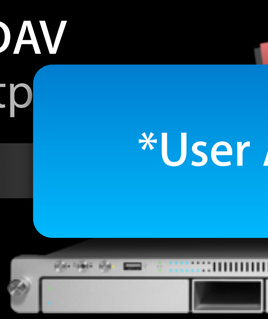
CalDAV
https

User on Whitelist

Mobile Access Server

63.x.y.z
ical.example.com

CalDAV
http



*User Authenticated

Origin Server
ical.example.com

# iCal and Address Book Services Via Mobile Access Server

External Network

Internal Network

CalDAV
https

Mobile Access Server

63.x.y.z
ical.example.com

CalDAV
http

Origin Server
ical.example.com

# Three Access Mechanisms

## HTTP/HTTPS

## IMAP/SMTP

# Three Access Mechanisms

# Mail Proxy

- Proxies IMAP mail commands
- Proxies SMTP mail commands
- Authenticates and Authorizes users at the proxy before allowing users access to servers

# Mail Proxy

External Network
(Internet)

Client

Proxy Mail Client

Proxy Mail Server

Internal Network
(Intranet)

Origin Server
mail.example.com

# Mail Services Via Mobile Access Server

External Network
(Internet)

Internal Network
(Intranet)

Mail
IMAP/SSL

Mobile Access Server

63.x.y.z
mailproxy.example.com

Origin Server
mail.example.com

# Mail Services Via Mobile Access Server

External Network
(Internet)

Internal Network
(Intranet)

Proxy Mail Server

Retrieve Mail

IMAP/SSL

*User Authenticated
*User on WhiteList

Proxy Client

Retrieve Mail

Mobile Access Server

63.x.y.z

mailproxy.example.com

Origin Server

mail.example.com

# Split DNS

External Network

ISP DNS

Client
http://wiki.example.com

Mobile Access Server

wiki.example.com = wiki.example.com

Internal Network

Internal DNS

Origin Server
wiki.example.com

# Split DNS

External Network

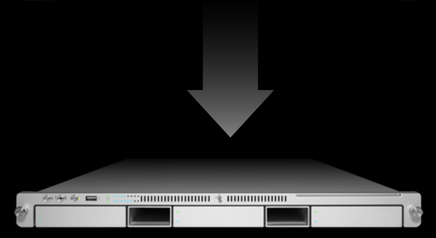
ISP DNS

Client
mailproxy.example.com

Mobile Access Server
mailproxy.example.com

Internal Network

Internal DNS



Origin Server
mail.example.com

Mail protocol does not support redirection

# Mail Client Configuration for Mobile Access

External Network

ISP DNS

**Client**
mailproxy.example.com

**Mobile Access Server**

Internal Network

Internal DNS

**Origin Server**
mail.example.com

# Configuration Demo

# Q&A

## WWDC Session Survey

You can rate your sessions on the WWDC Attendee Site.

Survey forms are located on each session description page at:

developer.apple.com/wwdc/attendee

# Summary

- Mobile Access Server provides secure, on-the-go access to web services, iCal server, Address Book server, and Mail server
- Configuration and administration is simple
- No client configuration is necessary
- Configuration of Split DNS is essential for deployment

# More Information

**Mark Malone**
Internet and Server Technologies Evangelist
mmalone@apple.com

**Apple Training and Certification**
http://training.apple.com

**Documentation**
Network Services Administration Guide
http://developer.apple.com/wwdc/attendee

# Related Sessions

| | |
|---|---|
| Contact Management with<br>Snow Leopard Server, Snow Leopard, and iPhone | Mission<br>Tuesday 10:30AM |
| Calendaring Solutions in<br>Snow Leopard Server, Snow Leopard, and iPhone | Mission<br>Tuesday 2:00PM |
| What's New for Wiki Server 2 | Mission<br>Thursday 10:30AM |

# Lab

| | |
|---|---|
| Mobile Access Lab | Information Technologies Lab<br>Wednesday 3:00PM |

WWDC09